REMARKS

Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1-38 are presently pending. Claims amended herein are 1, 6-10, 15, 21, 22, 26-28, and 30-38. Claims withdrawn or cancelled herein are none. New claims added herein are none.

Summary of Substance of Interview

[0003] Examiners Traore and Myhre graciously talked with me—the undersigned representative for the Applicant—on April 24, 2007. Applicant greatly appreciates the Examiners' willingness to talk. Such willingness is invaluable to all of us in our common goal of an expedited prosecution of this patent application.

[0004] During the interview, the Examiners indicated that although the office action failed to state § 101 rejections, unless amended, claim 1 and others would be rejected as directed to non-statutory subject matter.

[0005] During the interview, we discussed how the claims differed from the cited art, namely Menezes and Rosen. In particular, none of the cited art appears to address an identity matrix. Rosen discloses Warshall's Algorithm's, "zero-one matrices." Rosen/Warshall's zero-one matrix is not an identity matrix. Furthermore, none of the cited art appears to address a graph defined by a plurality of matrices wherein each of the vertices of the graph is represented by a corresponding matrix—the matrices describe the graph. As noted above, Rosen discloses Warshall's Algorithm, which is a way to find which vertex is connected to other vertices. The matrix presenting in Warshall's Algorithm represents the entire graph, not a vertex of the graph. Finally, none of the cited art appears to address tracing a path defined by a sequence of elements within an input block. As noted above, Rosen discloses Warshall's Algorithm, which deals with an adjacency matrix in a graph, describing all edges in the graph simultaneously. Warshall's matrix does not define a sequence of elements in an input block. Without conceding the propriety of the rejections and in the interest of expediting prosecution, I also proposed several possible clarifying amendments.

[0006] The Examiners were receptive to the proposals, and I understood the Examiners to indicate that proposed clarifying claim amendments appeared to distinguish over the cited art of record. For example, the Examiners indicated that clarification regarding claim 22, "labeling each node with a matrix, wherein the nodes make up a graph;" distinguished claim 22 over the cited art, namely Menezes and Rosen.

[0007] I understood the Examiners to tentatively agree that independent claim 15 would be patentable over the cited art as discussed during the interview. However, the Examiner indicated that she would need to review the cited art more carefully and do another search.

[0008] Applicant herein amends the claims in the manner discussed during the interview. Accordingly, Applicant submits that the pending claims are allowable over the cited art of record for at least the reasons discussed during the interview.

Formal Request for an Interview

[0009] If the Examiner's reply to this communication is anything other than allowance of all pending claims, then I formally request an interview with the Examiner. I encourage the Examiner to call me—the undersigned representative for the Applicant—

so that we can talk about this matter so as to resolve any outstanding issues quickly and efficiently over the phone.

[0010] Please contact me or my assistant to schedule a date and time for a telephone interview that is most convenient for both of us. While email works great for us, I welcome your call to either of us as well. Our contact information may be found on the last page of this response.

Claim Amendments and Additions

Without conceding the propriety of the rejections herein and in the interest of expediting prosecution, Applicant amends claims 1, 6-10, 15, 21, 22, 26-28, and 30-38, herein. Applicant amends claims in accordance with our telephone discussion with the examiner. Such amendments are made to expedite prosecution and quickly identify allowable subject matter. Such amendments are merely intended to clarify the claimed features, and should not be construed as further limiting the claimed invention in response to cited prior art.

Formal Matters

[0011] This section addresses any formal matters raised by the Examiner.

Specification

[0012] Under 35 U.S.C. 112, first paragraph, the Examiner rejects (objects to) paragraph 23 of the specification for "unclear, inexact or verbose terms used in the specification" (p. 3-4). Herein, Applicant amends the paragraph, as shown above, to correct the informality noted by the Examiner.

Claims

[0013] The Examiner notes that claims 27 and 29 invoke 35 U.S.C. 112, 6th paragraph by using "means-plus-function" language (p. 3). However, the Examiner further indicates that because she did not see "specific structural limitations disclosed in the specification" other than program modules (p. 3), she did not consider 35 U.S.C. 112, 6th paragraph invoked when examining claims 27 and 29. Applicant respectfully submits that sufficient structural features are disclosed for invoking 35 U.S.C. 112, paragraph 6 in the Specification in at least paragraph [00109] and Figure 6. Applicant respectfully requests the Examiner consider at least [00109] and Fig. 6, while further prosecuting this case. Applicant respectfully requests that the rejections of claims 27 and 29 be withdrawn, and the claims, as they properly invoke 35 U.S.C. 112, 6th paragraph, be examined.

[0014] The Examiner objects to claims 21 and 26 under 37 C.F.R. §1.75(c) for being of improper dependent form for failing to further limit the subject mater of a previous claim (p. 2). In support of the objection, the Examiner states that "Since Claims 15 and 22 (the parent claims) are method claims comprising a couple of steps and Claims 21 and 26 fail to add, delete, or change any of these steps, Claims 21 and 26 fail to further limit the parent claim."

Applicant respectfully submits that claims 21 and 26 are similar to an acceptable product-by-process claim in that they define a computer-readable medium having computer-executable instructions which direct a computer to perform the methods set forth in claims 15 and 22, respectively. The methods are thus physically embodied in a computer-readable medium. Claims 21 and 26 are proper in their construction in that they reference and are dependent from previous claims 15 and 22, and still further define the product created having embodied thereon the methods in claims 15 and 22. Moreover, the metes and bounds of claims 21 and 26 are clearly set forth in the methods of claims 15 and 22 from which claims 21 and 26 depend, respectively.

The fourth paragraph of 35 U.S.C. §112 requires "a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed." Claims 21 and 26 satisfy this statutory requirement. Claims 21 and 26 are written in a format that defines, in dependent form, a computer-readable medium to perform a method, thus enabling the performance of the methods set forth in claims 15 and 22, respectively.

The format of claiming a computer-readable medium with instructions to perform a method, or a computer programmed to perform the method, was approved in *In re Beauregard*, 35 USPQ2d 1383 (Fed. Cir. 1995). The primary difference between the *Beauregard* claims and claims 21 and 26 is that these claims are written in a dependent format. Often this format raises an initial concern because the preambles of the dependent claims differ from the base claims. However, the present dependent claims also comply with a format approved by the Board of Patent Appeals and Interferences in *Ex parte Adrianus P.M.M. Moelands*, 3 USPQ2d 1474 (PTO Board of Pat App and Int 1987). In *Moelands*, the Board upheld as appropriate the following dependent claim to a data transmission system:

> 11. A data transmission system comprising:
> at least two of the data transmission stations of claim 10;
> a clock bus interconnecting the clock terminals of the stations; and
> means which maintain the clock bus at the second voltage level in the absence of forcing by the stations.

Although the preamble in *Moelands*' claim 11 to a "data transmission system" is different than the preamble in claim 10 to a "data transmission station", the Board held that this dependent claim format satisfies the statutory requirements of both the second and fourth paragraphs of 35 U.S.C. §112.

[0015] Accordingly, claims 21 and 26 are in an acceptable dependent format and are in condition for allowance. Applicant respectfully requests that the objection to claims 21 and 26 be withdrawn.

Double-Patenting or Duplicate Claim Rejection

[0016] The Examiner rejects claims 3 and 7 as substantially duplicate claims. In light of the amendments presented herein, Applicant submits that this rejection is moot. Accordingly, Applicant asks the Examiner to withdraw this rejection.

Substantive Matters

Claim Rejections under § 112

[0017] Claim 22 is rejected under 35 U.S.C. § 112, 2nd ¶. In light of the amendments presented herein, Applicant submits that this rejection is moot. Accordingly, Applicant asks the Examiner to withdraw this rejection.

Anticipated Claim Rejections under § 101

[0018] During the telephone discussion on April 24, 2007, Examiners Traore and Myhre indicated that all independent claims except 15 should have been rejected under 35 U.S.C. 101. Applicant appreciates the Examiners' candor regarding this oversight. In light of the amendments presented herein, Applicant respectfully submits that all claims comply with the patentability requirements of § 101. The Applicant further asserts that these claims are allowable.

[0019] If the Examiner makes a rejection of the claims, then the Applicant requests additional guidance as to what is necessary to overcome the rejection.

Claim Rejections under §§ 102 and/or 103

[0020] Claims 1-38 are rejected under 35 U.S.C. § 102 and/or § 103. In light of the amendments presented herein and the decisions/agreements reached during the above-discussed Examiner interview, Applicant submits that these rejections are moot. Accordingly, Applicant asks the Examiner to withdraw these rejections.

[0021] The Examiner rejects claims 1-5, 7, 8, 31-35, 37, and 38; and 9, 11, 12, 22, and 26 under §102. For the reasons set forth below, the Examiner has not shown that cited references anticipate the rejected claims.

[0022] In addition, the Examiner rejects claims 10, 13, 14-21, and 23-25 under §103. For the reasons set forth below, the Examiner has not made a prima facia case showing that the rejected claims are obvious.

[0023] Accordingly, Applicant respectfully requests that the § 102 and/or § 103 rejections be withdrawn and the case be passed along to issuance.

[0024] The Examiner's rejections are based upon the following references alone and/or in combination:

- **Menezes**:Menezes, et al.; *Handbook of Applied Cryptography*, p. 332, ISBN 0-8493-8523-7;
- **Rosen:** Rosen; *Discrete Mathematics and Its Applications*, Second Ed., pp. 331-332, 367-375, 429-430, 432-434; American Telephone and Telegraph Company. USA (1991), ISBN 0-07-053744-5;
- **Aiello:** Aiello et al.; *Method and Apparatus for Generating Secure Hash Functions*, U.S. Patent 5,892,829.

Overview of the Application

[0025] The Application describes a technology for efficiently implementing secure hash functions and/or stream ciphers. More specifically, a family of graphs is described that has relatively large girth, large claw, and/or rapid mixing properties. The graphs are suitable for construction of cryptographic primitives such as collision resistant hash functions and stream ciphers, which allow efficient software implementation.

Cited References

[0026] The Examiner cites Menezes, Rosen and Aiello as primary references in anticipation- and/or obviousness-based rejections. The Examiner cites Menezes and Rosen as secondary reference in obviousness-based rejections.

Menezes

[0027] Menezes, a book on the topic of applied cryptography describes a general model for iterated hash functions.

Rosen

[0028] Rosen, a book on the topic of discrete mathematics and its applications describes Warshall's Algorithm.

Aiello

[0029] Aiello describes a technology for providing a secure hash function using a stretch function and a compression function.

Discussion of Cited Art

[0030] Applicant submits that the art rejections are not valid because, for each rejected claim, the cited references fail to disclose each and every element of that rejected claim.

§ 102(b) based upon Menezes

[0031] The Examiner rejects claims 1-5, 7, 8, 31-35, 37, and 38 under 35 U.S.C. § 102(b) as being anticipated by Menezes. Applicant respectfully traverses the rejections of these claims. Based on the reasons given below, Applicant asks the Examiner to withdraw the rejections of these claims.

§ 102(b) based upon Rosen

[0032] The Examiner rejects claims 9, 11, 12, 22, and 26 under 35 U.S.C. § 102(b) as being anticipated by Rosen. Applicant respectfully traverses the rejections of these claims. Based on the reasons given below, Applicant asks the Examiner to withdraw the rejections of these claims.

§ 103(a) based upon Rosen

[0033] The Examiner rejects claim 13 under 35 U.S.C. § 103(a) as being obvious over Rosen. Applicant respectfully traverses the rejections of these claims. Based on the reasons given below, Applicant asks the Examiner to withdraw the rejections of these claims.

[0034] The Examiner rejects claims 10, 14-21, and 23-25 under 35 U.S.C. § 103(a) as being obvious over Rosen in view of Menezes. Applicant respectfully traverses the rejections of these claims. Based on the reasons given below, Applicant asks the Examiner to withdraw the rejections of these claims.

§ 103(a) based upon Menezes

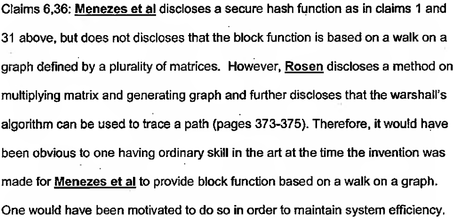
[0035] The Examiner rejects claims 6 and 36 under 35 U.S.C. § 103(a) as being obvious over Menezes in view of Rosen. Applicant respectfully traverses the rejections of these claims. Based on the reasons given below, Applicant asks the Examiner to withdraw the rejections of these claims.

§ 103(a) based upon Aiello

[0036] The Examiner rejects claims 27-30 under 35 U.S.C. § 103(a) as being obvious over Aiello in view of Menezes. Applicant respectfully traverses the rejections of these claims. Based on the reasons given below, Applicant asks the Examiner to withdraw the rejections of these claims.

Independent Claims 1, 27, and 31

[0037] The Examiner indicates (Action p. 4) that claims 1 and 31 are anticipated by Menezes (fig. 9.2 a and b; p. 332), and that claim 27 is obvious over Aiello in view of Menezes (Action p.15). The Examiner further indicates (Action p. 14) that claims 6 and 36 are obvious over Menezes in view of Rosen:



> Claims 6,36: Menezes et al discloses a secure hash function as in claims 1 and 31 above, but does not discloses that the block function is based on a walk on a graph defined by a plurality of matrices. However, Rosen discloses a method on multiplying matrix and generating graph and further discloses that the warshall's algorithm can be used to trace a path (pages 373-375). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for Menezes et al to provide block function based on a walk on a graph. One would have been motivated to do so in order to maintain system efficiency.

[0038] Applicant submits that neither Menezes nor Rosen nor Aiello alone or in combination anticipate or make obvious claims 1, 27, or 31 as amended because they fail to disclose each and every element and feature of these claims. For example, at least the following elements as recited in claim 1 (with emphasis added) are not disclosed:

> applying **a block function** to a first data input block from a plurality of data input blocks, wherein the block function comprises a walk on **a graph defined by a plurality of matrices**
>
> . . .
>
> **providing the hash value of the plurality of input blocks to a computing environment** wherein the hash value facilitates more efficient or more secure data encryption.

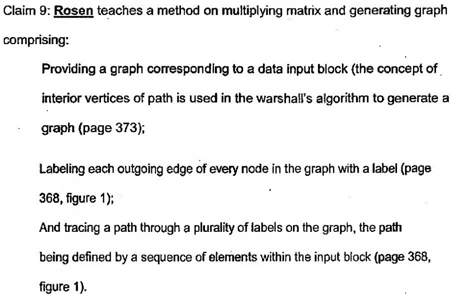
[0039] Claims 1, 27, and 31 recite a block function acting upon data input blocks based on a walk on a graph described by a plurality of matrices. Menezes, Rosen, and

Aiello do not. Rather, Menezes discloses "a general model for iterated hash functions," Rosen discloses Warshall's Algorithm, "an efficient method for computing the transitive closure of a relation," and Aiello teaches against block ciphers (c. 2 ll. 1-10), disclosing stretch functions used in combination with compression functions Each matrix in claim 1 represents a vertex of the graph—the matrices describe the graph. Warshall's Algorithm is a way to find which vertex is connected to other vertices. The matrix presented in Warshall, represents the entire graph, not a vertex of the graph.

[0040] Applicant respectfully submits that, for at least the foregoing reasons, these claims are allowable, and asks the Examiner to withdraw the rejections of these claims.

Independent Claim 9

[0041] The Examiner indicates (Action pp. 6-7) that claim 9 is anticipated by Rosen (p. 368 and p. 373).



Claim 9: Rosen teaches a method on multiplying matrix and generating graph comprising:

Providing a graph corresponding to a data input block (the concept of interior vertices of path is used in the warshall's algorithm to generate a graph (page 373);

Labeling each outgoing edge of every node in the graph with a label (page 368, figure 1);

And tracing a path through a plurality of labels on the graph, the path being defined by a sequence of elements within the input block (page 368, figure 1).

[0042] Applicant submits neither Rosen nor Menezes alone or in combination anticipate or make obvious this claim as amended because they fail to disclose each and every element and feature of this claim. For example, at least the following elements as recited in this claim (with emphasis added) are not disclosed:

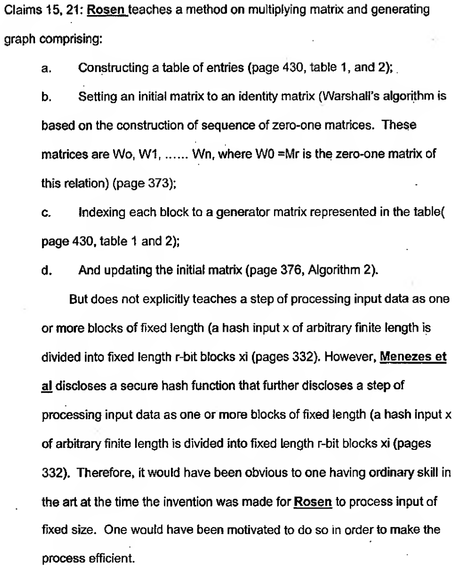
> tracing a path through a plurality of labels on the graph, the path being defined by **a sequence of elements within the input block**; and
>
> using the **tracing of the path for encryption in a computing environment** wherein the **tracing of the path through the plurality of labels** facilitates more efficient or more secure **data encryption.**

[0043] Claim 9 recites tracing a path that is "defined by a sequence of elements within an input block." Both Menezes et al. and Rosen do not. Rather, Rosen, through Warshall's Algorithm, deals with an adjacency matrix in a graph, describing all edges in the group simultaneously. Warshall's matrix does not define a sequence of elements in an input block. Additionally, neither cited reference discloses tracing a path in a computing environment for encryption.

[0044] Applicant respectfully submits that, for at least the foregoing reasons, this claim is allowable, and asks the Examiner to withdraw the rejection of this claim.

Independent Claim 15

[0045] The Examiner indicates (Action pp. 10-11) that claim 15 is anticipated by Rosen (p. 332, p. 373, p. 376 (not provided), and p. 430).



Claims 15, 21: **Rosen** teaches a method on multiplying matrix and generating graph comprising:

a. Constructing a table of entries (page 430, table 1, and 2);

b. Setting an initial matrix to an identity matrix (Warshall's algorithm is based on the construction of sequence of zero-one matrices. These matrices are Wo, W1, ... Wn, where W0 =Mr is the zero-one matrix of this relation) (page 373);

c. Indexing each block to a generator matrix represented in the table(page 430, table 1 and 2);

d. And updating the initial matrix (page 376, Algorithm 2).

But does not explicitly teaches a step of processing input data as one or more blocks of fixed length (a hash input x of arbitrary finite length is divided into fixed length r-bit blocks xi (pages 332). However, **Menezes et al** discloses a secure hash function that further discloses a step of processing input data as one or more blocks of fixed length (a hash input x of arbitrary finite length is divided into fixed length r-bit blocks xi (pages 332). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for **Rosen** to process input of fixed size. One would have been motivated to do so in order to make the process efficient.

[0046] Applicant submits neither Rosen nor Menezes alone or in combination anticipate or make obvious claim 15 as amended because they fail to disclose each and every element and feature of this claim. For example, at least the following elements as recited in this claim (with emphasis added) are not disclosed:

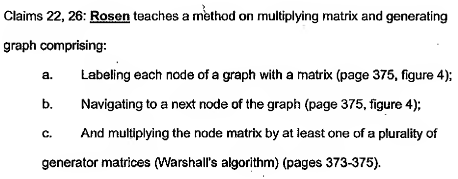
> **setting an initial matrix to an identity matrix;**
>
> . . .
>
> **updating the initial matrix.**

[0047] Claim 15 recites "setting an initial matrix to an identity matrix." An identity matrix is a square matrix with 1s on the main diagonal, and 0s in all other positions. Both Menezes et al. and Rosen do not disclose an identity matrix. Rather, Rosen, discloses Warshall's Algorithm, "based on construction of a sequence of zero-one matrices." Because it can have any of the entries as zero or one, Warshall's zero-one matrix is not an identity matrix. Additionally, the page of the reference cited to anticipate updating the initial matrix was not provided.

[0048] Applicant respectfully submits that, for at least the foregoing reasons, this claim is allowable, and asks the Examiner to withdraw the rejection of this claim.

Independent Claim 22

[0049] The Examiner indicates (Action p. 7) that claim 22 is anticipated by Rosen (pp. 373-375 and fig. 4).



Claims 22, 26: **Rosen** teaches a method on multiplying matrix and generating graph comprising:

a. Labeling each node of a graph with a matrix (page 375, figure 4);

b. Navigating to a next node of the graph (page 375, figure 4);

c. And multiplying the node matrix by at least one of a plurality of generator matrices (Warshall's algorithm) (pages 373-375).

[0050] Applicant submits neither Rosen nor Menezes alone or in combination anticipate or make obvious this claim as amended because they fail to disclose each and every element and feature of this claim. For example, at least the following elements as recited in this claim (with emphasis added) are not disclosed:

> **labeling each** of a plurality of **nodes** with a **matrix**, wherein the plurality of nodes make up a graph;
>
> . . .
>
> **multiplying each node matrix by at least one** of a plurality of **generator matrices**; and

[0051] Claim 22 recites "labeling each node of a graph with a matrix." As indicated regarding claim 1, above, both Menezes et al. and Rosen do not. The matrix presented in Warshall, represents the entire graph, not a vertex (node) of the graph. Additionally, neither cited reference discloses multiplying a node matrix by a generator matrix.

[0052] Applicant respectfully submits that, for at least the foregoing reasons, this claim is allowable, and asks the Examiner to withdraw the rejection of this claim.

Dependent Claims

In addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

Obviousness

[0053] In addition to the cited art failing to disclose each and every element of the rejected claims, Applicant disagrees with the Examiner's obviousness rejections. Applicant requests the Examiner's assistance to help me understand how to combine the cited references without the benefit of piecemeal consideration, hindsight reasoning, or using the Applicant's claims to acquire motivations to obtain the claimed results.

[0054] The Examiner states that her motivations include:

- "for Rosen to indicate the hash value to be the last value of the iteration . . . in order to maintain data integrity," (Action, p. 9 re: claim 10);
- "for Rosen to divide the input string in input blocks . . . in order to maintain data integrity," (Action, pp. 9-10 re: claim 14);
- "for Rosen to process input of fixed size . . . to make the process efficient," (Action, pp. 10-11 re: claims 15 and 21);

- "for Rosen to include a secure hash function . . . to maintain data integrity," (Action, p. 11 re: claim 16);

- "for Menezes [Rosen] to use DES . . . to maintain data integrity," (Action, p. 11 re: claim 17);

- "for Menezes to use matrix multiplication for updating purpose . . . to maintain system efficiency," (Action, p. 12 re: claims 18 and 19);

- "for Rosen to provide a stream cipher . . . to maintain data integrity," (Action, pp. 12-13 re: claims 23 and 24);

- "for Rosen and Menezes to provide generator matrices with a free monoid properties . . . to maintain data integrity," (Action, pp. 13-14 re: claims 20 and 25);

- "for Menezes to provide block function based on a walk on a graph . . . to maintain system efficiency," (Action, p. 14, re: claims 6 and 36);

- "for Aiello to include a means for applying a flock function to a first and second data input block from a plurality of data input blocks . . to maintain data integrity," (Action, pp. 15-16, re: claims 28 and 29);

- "for Aiello to include a means dividing the input string to a plurality of data input blocks . . to maintain data integrity." (Action, pp. 16-17 re: claim 30).

[0055] The above quotes appear to support that the Examiner used piecemeal consideration, hindsight reasoning, and the Applicant's disclosure to provide sought after motivations to combine references.

[0056] Furthermore, at least in the case of claims 20 and 25, the Applicant is unable to locate the features cited in the purported motivation in the cited references.

[0057] For at least these reasons, Applicant respectfully requests that the Examiner withdraw the obviousness rejections of the above cited claims.

[0058] Regarding claim 13, Applicant has a hard time understanding how a suggestion, teaching, or motivation for one of ordinary skill in the art at the time of the invention (hereinafter "OOSA") or from the common knowledge of OOSA to have modified Rosen in order to obtain the method of claim 13 is reached. As best understood by the Applicant the Examiner attempted to invoke common knowledge of an OOSA to render claim 13 obvious.

[0059] Although the subject matter of the specification cannot be read into the claims, the claims should be interpreted in light of the specification. Regarding claim 13, it seems that the Examiner did not interpret the claim in light of the specification. "Degree of a graph" has a separate meaning from degree of an angle, with which the Examiner apparently equated it. Degree of a graph is well known to those in the art to refer to a function of the number of edges incident to the vertices of a graph.

[0060] Applicant does not understand how it is sufficient to establish a prima facie case of obviousness for the Examiner to say that she "considers it is immaterial to compare the integer value and the degree of the graph." The Examiner presents the following statement of motivation, "It would have been obvious to one having ordinary skills in the art at the time the invention was made to make the angle smaller than the value of the labels. One would have been motivated to do so in order to maintain data integrity since small angle are used in trigonometry to control function in order to reduce the error rate."

[0061] However, Applicant submits that Rosen never teaches, discloses, suggests or hints at *angles smaller than the value of labels* or *small angles used in trigonometry to control function in order to reduce the error rate.* The problem solved by Rosen relates to closures of relations. Applicant submits that this problem does not imply *angles smaller than the value of labels* or *small angles used in trigonometry to control function in order to reduce the error rate.* It also does not suggest using the degree of a graph to set forth integer labels of nodes to be used for encryption, as this claims does.

[0062] For at least these reasons, Applicant respectfully requests that the Examiner withdraw the rejection of claim 13.

Conclusion

[0063] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action**. Please call/email me or my assistant at your convenience.

Respectfully Submitted,

Dated: 05/07/2007

By:

Bea Koempel-Thomas
Reg. No. 58,213
(509) 324-9256 x259
bea@leehayes.com
www.leehayes.com

My Assistant: Carly Bokarica
(509) 324-9256 x264
carly@leehayes.com